Datainspektionen

Yttrande
2018-03-06

Diarienr
2725-2017

Ert diarienr
Ju2017/08898

Justitiedepartementet
103 33 Stockholm

Hemlig dataavläsning - ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89)

Datainspektionen har granskat betänkandet huvudsakligen utifrån myndighetens uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter.

Datainspektionen avstyrker utredningens förslag till utformning och möjlighet att använda tvångsmedlet hemlig dataavläsning.

Generella synpunkter på betänkandet

De hemliga tvångsmedlen intar en särställning på integritetsskyddområdet eftersom de ger staten en laglig rätt till en långtgående och ofta djupt integritetskränkande övervakning och kontroll över medborgarna.[1]

Användningen av det föreslagna tvångsmedlet hemlig dataavläsning kan komma att innebära ett i den personliga integriteten synnerligen ingripande intrång. För att införa ett sådant tvångsmedel i ett demokratiskt samhälle måste det föreligga mycket starka skäl.

Eftersom varje tvångsmedel och övervakning av enskilda personer innefattar ett integritetsintrång måste nödvändigheten av dessa metoder alltid vägas mot integritetsskyddsintresset. Vid dessa bedömningar måste hänsyn tas till kraven i regeringsformen, Europakonventionen och EU:s rättighetsstadga. Enskildas rätt till skydd för sitt privat- och familjeliv och sitt hem och sin korrespondens är en grundläggande rättighet i ett demokratiskt samhälle. Varje inskränkning i denna rätt måste bygga på ett angeläget samhälleligt behov av inskränkning och den måste stå i rimlig proportion till det syfte som

[1] Se SOU 2007:22 del 1 s. 170.

Postadress: Box 8114, 104 20 Stockholm
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00

ska tillgodoses genom ingreppet. Vidare måste undantagen vara utformade med sådan precision att inskränkningen av rättigheten är förutsägbar i rimlig utsträckning. Vid bedömningen av om det föreligger ett behov av ett nytt tvångsmedel spelar frågan om effektivitet och det praktiska värdet av det en stor roll.

Som utredningen konstaterar kan förslaget till hemlig dataavläsning, om alla de uppgifter som skulle kunna tillgängliggöras alltid samlas in i ett sammanhang genom ett enda tillstånd, bli väsentligt kraftfullare än något av de befintliga hemliga tvångsmedlen. Det skulle, vid ett införande i enlighet med utredningens förslag, kunna vara möjligt för den brottsbekämpande myndigheten som använder metoden att närmast fullständigt kunna kartlägga och övervaka den person som utsätts för åtgärden. En sådan totalövervakning av en person innebär naturligtvis synnerligen stora risker för den personliga integriteten för den som utsätts för åtgärden, och ibland även för andra.

Lagar som inskränker integritetsskyddet får endast genomföras om det intresse som ska tillgodoses är så starkt och integritetsskyddsintresset så förhållandevis svagt att inskränkningen framstår som proportionerlig.

Sammanfattningsvis anser Datainspektionen att utredningen föreslagit ett tvångsmedel som är synnerligen ingripande i enskildas personliga integritet. Nödvändigheten av den föreslagna utformningen och användningen av tvångsmedlet måste anses väsentligt understiga integritetsskyddsintresset. Mot denna bakgrund avstyrker Datainspektionen förslaget.

Åtgärder för att förbättra integritetsanalysen och andra väsentliga krav på förstärkningar av integritetsskyddet

Datainspektionen anser att den metod för integritetsanalys som utredningen redovisar i kapitel 9 är en bra utgångspunkt. En grundlig genomgång är en förutsättning för att kunna bedöma om förslaget till ett nytt tvångsmedel uppfyller de krav som integritetsskyddslagstiftningen ställer.[2] Datainspektionen har dock synpunkter på analysen.

För det första har utredningen bort utreda och redovisa de brott för vilka hemlig dataavläsning kan vara aktuellt enligt förslaget. Här har utredningen

[2] Se integritetsskyddskommitténs sammanfattande analys, SOU 2007:22 s. 445 ff.

under behovsanalysen endast sammanfattat att det t.ex. finns tungt vägande behov, i förundersökningsfallen, avseende de brott som kan föranleda hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 § andra stycket rättegångsbalken. Datainspektionen hade velat se en prövning av behovet och proportionaliteten för vart och ett av brotten och anser, redan på befintligt underlag, att förslaget omfattar brott som inte kan anses tillräckligt allvarliga. Det sistnämnda gäller särskilt de brott som är aktuella genom hänvisningen till 27 kap. 18 § punkten 9 rättegångsbalken och som ger möjlighet att använda hemlig dataavläsning om det kan antas att straffvärdet överstiger två års fängelse.[3] Enligt Datainspektionens bedömning bör, som utgångspunkt, endast mycket allvarliga brott som kan påverka rikets säkerhet, såsom terroristbrott, och mycket grov organiserad brottslighet, kunna aktualisera ett så pass ingripande tvångsmedel.

För det andra anser Datainspektionen att utredningen, vid sin bedömning av integritetsriskerna i kapitel 9, genomgående och i betydande grad undervärderat dessa. Datainspektionen anser också att utredningen inte bort utgå från nuvarande risker som en normerande nivå och endast bedömt om riskerna kan anses högre i förhållande till denna nivå. Som exempel konstaterar utredningen att förslaget till hemlig dataavläsning för att ta del av innehåll i och uppgifter om meddelanden inte innebär någon ökad risk för den personliga integriteten. Datainspektionen gör en annan bedömning. Som exempel kan tas att en individ kan ha valt att kryptera en viss kommunikation med hänsyn till att kommunikationen innehåller känsliga uppgifter. Redan en möjlighet att ta del av dessa uppgifter med stöd av hemlig dataavläsning har en direkt påverkan av skyddet på den personliga integriteten, som måste värderas betydligt högre än vad utredningen gjort. Därtill anser inspektionen att utredningen också missat att en kombination av olika risker kan ge ytterligare skäl till att värdera dessa högre.

För det tredje anser inspektionen att frågan om jurisdiktion, särskilt avseende användarkonton, kommunikationstjänster och lagringstjänster enligt 1 § punkten 2 i lagförslaget, inte tillräckligt analyserats utifrån förväntad effektivitet med beaktande av den nuvarande svenska tillämpningen av territorialitetsprincipen. Redan idag finns det stora mängder av användare i Sverige som använder tjänster från t.ex. Facebook, Twitter, Apple, Microsoft och Amazon. Enligt Datainspektionens bedömning skulle stora mängder

[3] Se också Datainspektionens yttrande den 2 december 2005, dnr 1391-2005.

information lagrade i nyssnämnda företags tjänster fortfarande inte vara åtkomliga vid ett genomförande av utredningens förslag. Datainspektionens slutsats är därför att utredningens förslag i denna del inte kommer att bli effektivt. Frågan om jurisdiktion är komplex men det går inte att bortse från den vid bedömning av den förväntade effektiviteten av hemlig dataavläsning.

Vidare anser Datainspektionen att objektet för åtgärden måste preciseras. Datainspektionen har tidigare kritiserat begreppet informationssystem och framfört att detta inte är tillräckligt tydligt för att nå upp till regeringsformen och Europakonventionens krav.[4] Även om utredningen, i förhållande, till det tidigare förslaget, i viss mån preciserat begreppet anser Datainspektionen att det inte är tillräckligt tydligt och leder till en betydande osäkerhet om vad som omfattas.

Slutligen anser Datainspektionen att domstolens prövning måste förstärkas. Enligt förslaget kommer domstolen vid tillståndsprövningen inte kunna ta hänsyn till den teknik som den brottsbekämpande myndigheten vill använda för att verkställa tvångsmedlet. Datainspektionens bedömning är att det krävs kunskap om tekniken för att kunna göra en nödvändighets- och proportionalitetsbedömning i det enskilda fallet. Det bör därför införas ett krav på att ansökan om tillstånd ska innehålla sådana uppgifter. Dessutom bör inte åklagare kunna fatta interimistiska beslut om tillstånd till hemlig dataavläsning. Ett tillstånd bör alltid prövas av domstol med hänsyn till det synnerligen allvarliga intrång i enskilds personliga integritet som det kan innebära.

Behov av ett samordnat lagstiftningsarbete

I det fortsatta lagstiftningsarbetet vill Datainspektionen också framhålla vikten av att samordna lagstiftningsarbetet med andra förslag till åtgärder mot terrorism och annan allvarlig brottslighet som har konsekvenser för den personliga integriteten. Som exempel kan nämnas utredningen om datalagring och EU-rätten (SOU 2017:75), brottsdatalagen (SOU 2017:29), brottsdatalag – kompletterande lagstiftning (SOU 2017:74), utlandsspioneriutredningen (SOU 2017:70), utredningen om genomförande av vissa straffrättsliga åtgärder för att förhindra och bekämpa terrorism (SOU 2017:72) och lag om flygpassageraruppgifter (SOU 2017:57).

[4] Se Datainspektionens remissvar den 2 december 2005, dnr 1391-2005.

Synpunkter på valda delar av betänkandet

Datainspektionen lämnar i det följande närmare synpunkter på valda delar av kapitel 10 i utredningen.

10.2 Innebörden av hemlig dataavläsning

Som redan framförts ovan måste objektet för åtgärden preciseras.

10.5 Hemlig dataavläsning under förundersökning

Som redan framförts ovan ifrågasätter Datainspektionen att de alla de brott som utredningen föreslår ska kunna ge möjlighet att använda hemlig dataavläsning. Enligt inspektionens bedömning bör, som utgångspunkt, endast mycket allvarliga brott som kan påverka rikets säkerhet, såsom terroristbrott och mycket grov organiserad brottslighet, kunna aktualisera ett så pass ingripande tvångsmedel.

Datainspektionen konstaterar att avläsning eller upptagning av kameraövervaknings- eller rumsavlyssningsuppgifter begränsas till vissa platser enligt den modell som gäller idag. Utredningen har dock inte tillräckligt analyserat att det finns en betydande skillnad med förslaget jämfört med dagens tvångsmedel. Genom hemlig dataavläsning får den brottsbekämpande myndigheten möjlighet att t.ex. använda den misstänktes mobiltelefon för att avläsa eller ta upp uppgifter. Hur ska då den brottsbekämpande myndigheten kunna säkerställa att uppgifter avläses eller tas upp endast på platser som omfattas av tillståndet? Datainspektionen ser betydande integritetsrisker med förslaget och riskerna måste belysas i det fortsatta lagstiftningsarbetet.

Slutligen konstaterar Datainspektionen, i linje med att det kan vara svårt att identifiera ett visst informationssystem, att kan det vara svårt att kunna koppla ett visst informationssystem till den misstänkte i en förundersökning. Hur ska de brottsbekämpande myndigheterna kunna tillgodose rättssäkerheten i sådana situationer? Även detta behöver belysas ytterligare i det fortsatta lagstiftningsarbetet.

10.6 Hemlig dataavläsning i underrättelseverksamhet

På motsvarande sätt som under avsnitt 10.5 konstaterar Datainspektionen att det kan finnas svårigheter att koppla ett visst informationssystem till den som enligt utredningen kan bli föremål för hemlig dataavläsning i underrättelseverksamhet.

10.10 Genomförande av hemlig dataavläsning

Som framgår ovan är det enligt Datainspektionen det inte möjligt för en domstol, som har pröva om ett tillstånd till hemlig dataavläsnings ska medges, att göra en fullständig nödvändighets- och proportionalitetsbedömning i det enskilda fallet utan att det redovisas hur åtgärden ska genomföras rent tekniskt. Det bör därför enligt Datainspektionen införas krav på att en ansökan om tillstånd ska innehålla sådana uppgifter.

Datainspektionen delar utredningens bedömning att s.k. otillåten tilläggsinformation ska förstöras omedelbart.

10.11 Vissa andra rättssäkerhetsgarantier

Datainspektionen har tidigare kritiserat ett förslag till hemlig dataavläsning som bl.a. innefattat bestämmelser om att upptagningar eller uppteckningar vid hemlig dataavläsning ska granskas snarast möjligt.[5] Det som Datainspektionen då framförde äger alltjämt giltighet. Den föreslagna regleringen riskerar att medföra att en stor mängd uppgifter rutinmässigt bevaras under en längre tid. Med hänsyn till det föreslagna tvångsmedlets särskilt ingripande karaktär och de avsevärda integritetsrisker som är förknippade med detsamma, bör det införas uttryckliga regler som anger att uppgifter som inte är relevant för att utreda brott ska förstöras omedelbart efter att de har granskats.

10.12 Några särskilda frågor

Utredningen har, med viss tveksamhet, valt att inte ålägga operatörerna en skyldighet att medverka vid verkställighet av hemlig dataavläsning. Datainspektionen delar den uppfattning som experten Anne Ramberg, Advokatsamfundet, framför i sitt särskilda yttrande om det inte är en god lagstiftningsåtgärd att lagstifta kring en medverkansmöjlighet men underförstått uttala att operatörerna måste medverka för att den hemliga dataavläsningen ska kunna bli effektiv.[6]

[5] Se remissyttrande den 2 december 2005, dnr 1391-2005.
[6] Se det särskilda yttrandet s. 592.

Detta yttrande har beslutats av generaldirektören Lena Lindgren Schelin efter föredragning av juristen Jonas Agnvall. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom och t.f. enhetschefen Vilhelm Andersson deltagit.

Lena Lindgren Schelin

Jonas Agnvall